Author(s): Basnet, Sunil & Valdez Banda, Osiris Alejandro & Kujala, Pentti

Title: Review of the safety engineering techniques for a complex ship system

Year: 2018

Version: Final published version

Please cite the original version:

Basnet, Sunil & Valdez Banda, Osiris Alejandro & Kujala, Pentti. 2018. Review of the safety engineering techniques for a complex ship system. The 7th Asia Conference on Earthquake Engineering. 10.

Review of the safety engineering techniques for a complex ship system

Sunil Basnet
Marine Department
Aalto University
Espoo, Finland
sunil.basnet@aalto.fi

Osiris A. Valdez Banda
Marine Department
Aalto University
Espoo, Finland
osiris.valdez.banda@aalto.fi

Pentti Kujala
Marine Department
Aalto University
Espoo, Finland
pentti.kujala@aalto.fi

***Abstract*— Marine industry is leaning towards the autonomous vessels; and advanced technologies are being developed for autonomous operations. However, this rapid technological change has increased the level of complexity in ship systems. As the interactions between components are increasing further and software are getting imbedded into components, the nature of risks in modern systems can be different than in the traditional systems; where the risks were mostly limited to human errors and component failures. However, for identifying risks in modern systems, it is first important to understand the system composition and the behavior of components. Since traditional system-safety engineering techniques, developed for the relatively simpler systems in past, are still dominant in marine industry. These techniques may not be able to cope with the risks due to increasing complexity.**

This paper reviews and identifies a suitable modelling approach and a risk analysis method for a complex ship system. A modern modeling approach known as Systems-Modeling Language (SysML) and a modern risk analysis method known as Systems-Theoretical Process Analysis (STPA) are reviewed and compared with widely used traditional methods known as the Tree structure method and Fault Tree Analysis. SysML is a graphical modeling language that presents structural composition, component functions, behavior, constraints and requirements of a complex system. STPA is a risk analysis method that aims to identify and mitigate risks in a complex system. The review and comparison results are presented in the paper.

The results of this study suggest that the modern methods are more suitable than the traditional methods when the functionality of each method are considered. However, as the modern methods are more detailed, and are focused on the functionality, they are relatively complex and require more resources for the analysis in comparison to the traditional methods. Some viable solutions to improve the drawbacks of SysML and STPA, and possible future research topics are presented.

Keywords—STPA, SysML, FTA, Tree structure method, complex systems, safety engineering techniques.

I. INTRODUCTION

A. Research background

Autonomous vehicles are already the state of the art for roadways and airways. However, autonomous ships are still in the early phase of development. Nevertheless, after the initial feasibility study project, Maritime Unmanned Navigation through Intelligence in Networks (MUNIN), companies such as Rolls-Royce, Kongsberg and Vigor Industrial have already initiated projects to construct autonomous ships; and are set to mark the beginning of a new era of shipping in the near future. Autonomous vessels have attracted several marine professionals and companies, as they have the potential to improve the sustainability of the marine transport industry by reducing the environmental impacts, operational expenses and the shortage of seagoing professionals [1]. Thus, for autonomous operations, advanced features in ship systems such as advanced navigation and sensor fusion are being developed [2] [1]. As a result, the level of complexity in the ship system is increasing further.

Although, the technologies in ship systems are advancing at a faster pace, system safety engineering techniques are lagging far behind. Traditional risk analysis methods such as Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) are still widely used for identifying risks in modern marine vessels. These methods were developed several decades ago for relatively simpler systems; and they were effective at past because of their ability to analyze the system by isolating and simplifying the interfaces between system components [3]. Unlike traditional systems, components in modern systems cannot be treated independent, as the interactions among components are increasing and software are being embedded in components and sub systems. As a result, it is unsurprising that the nature of accidents is also changing [3]. There is a possibility that traditional methods may not identify these emerging risks. Hence, a review of modern and traditional methods for risk analysis is important for future projects.

However, for identifying risks in a complex system, it is first important to understand the system itself. Since, the interactions among components are growing, understanding how the component interacts to perform activities or functions is crucial. Furthermore, the analysts must also understand how components are interconnected for identifying risks in a system. With better understanding of the system, the risk analysis methods will then be more effective. Moreover, these models can help operators to operate the system efficiently; and allows designers or analysts to understand the system for improving the future system designs. In addition, models can also be used to guide the design process through the requirements analysis of the system. Thus, a modeling approach that can present the overview of a complex ship system is as crucial as the risk analysis method; and a suitable modeling approach for complex ship system needs to be identified and implemented.

B. Research objectives

The aim of this research is to identify a suitable modeling approach and a risk analysis method for a complex ship system. Thus, for achieving the aim, a widely used traditional method will be compared with a modern method developed for a complex system.

This paper should aim to answer following research questions:

1. Which approach is suitable for modeling a complex ship system?
2. Which method is suitable for identifying risks in a complex ship system?

C. Research limitations

As the scope of this research is wide, following limitations have been considered:

1. Only two modeling approaches and two risk analysis methods are selected for review and comparison.
2. The following simplifications were made on the methods:
    a. A simplified version of SysML labelled as SysML-lite has been used for the review in this paper. (more information on the review chapter)
    b. Deriving cut sets for failures in FTA has not been considered in the review.
3. Due to the lack of data about the failure in a complex ship system, probabilistic methods are not considered.

II. METHODOLOGY

A. Review of modelling approaches

1) Introduction and selection of methods

Modelling approaches aim to provide the overview of a system through different models. These models are required to understand the system as they present the composition of the system, and interactions and behavior of the system components. As the systems in past were relatively simpler with low component interactions and were easier to understand, modelling approaches for physical systems were not much developed. However, the increased complexity in modern systems has led to the realization of the importance of modelling approaches. As a result, some modelling approaches for the complex systems were developed recently.

The only traditional modeling approach that is being widely used is the Tree structure method, which only presents a structure of a system in a hierarchical approach. Furthermore, texts are used to explain the system properties and functions in the specification documents. On the other hand, there are two modeling approaches developed recently for complex systems known as Object-Process Methodology (OPM) and Systems Modeling Language (SysML).

a) Object-Process Methodology (OPM)

OPM is a modeling approach that aims to model complex systems in a holistic approach. It presents the structural composition, the behavioral and the functional aspects of the system in a single diagram. In addition to a graphical model, it also includes textual representations for better understanding about the system. [4]

b) Systems Modeling Language (SysML)

SysML is a general-purpose modeling language, which supports the analysis, design, verification, specification and validation of complex systems. It includes nine different types of diagrams to present the structure, behavior, and requirements of the system. Furthermore, it also provides support for the engineering analysis of a system with a parametric diagram. [5]

c) General comparison and selection of methods for the review.

OPM and SysML, both were developed to model complex systems. OPM aims to present an overview of a complex system with a single diagram and texts. SysML on the other hand, present diagrams of nine different kind for the same purpose. A general comparison between these methods is presented in Table 1.

Table 1. A general comparison between OPM and SysML.

Question	OPM	SysML
Does it model the structural composition of a system?	Yes	Yes
Does it model the behavior of a system?	Yes	Yes
Does it present the requirements of a system?	No	Yes
Does it provide any tool for the engineering analysis of the system?	No	Yes
Structure of a model	A single diagram and texts	Diagrams of 9 different kind

Although both methods manage to present the structure and behavior of complex systems, SysML presents the requirements of systems and supports analysts for performing the engineering analysis of a system, which is lacking in OPM [4]. Furthermore, Modern vessel usually consists of several complex systems. Thus, a single type of diagram for modeling the structure and behavior of the system can be difficult and complex to manage.

Based on the comparison and initial review, SysML and the Tree structure method are selected for reviewing.

2) The Tree structure method review

The Tree structure method is one of the widely used traditional modeling approaches which presents a graphical model of the composition of a system. In this model, the system is classified into subsystems and components in a hierarchy, which resembles like a tree. A tree structure starts with a single source or edge and the classification is shown with branches that develop along nodes [6]. Each element of the tree such as systems, sub-systems and components are represented as nodes and are connected with a solid line.

In the Tree structure method, the system is placed in the first level node of the tree. The system is then classified into sub systems in the second level. The sub systems are further

classified into components and the level continues further as required. A classification of a propulsion plant in an offshore patrol vessel presented in [7] is shown in Figure 1.

Moreover, this approach has also been adapted to various fields. For example, FTA uses this structure to classify faults and processes by adding this structure with Boolean logic gates and different node types. Similarly, decision trees used in machine learning also utilizes tree structure for classifying decisions. Hence, it is utilized widely in different fields where there is a need to show the classification of a system, event and data into further details in a simple manner.

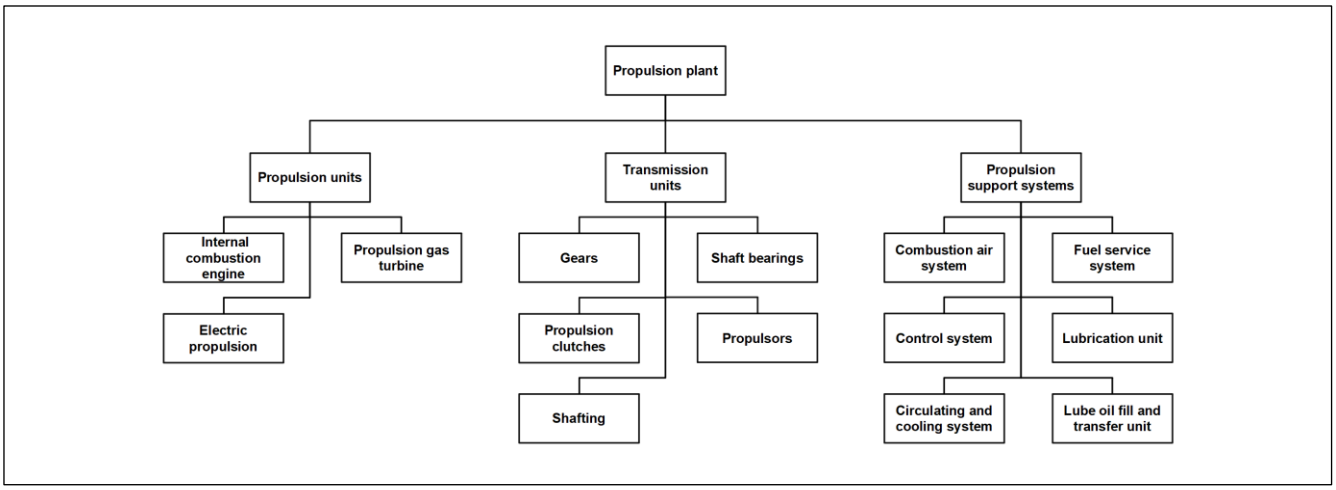


Figure 1. A classification of a propulsion plant in an offshore patrol vessel using the Tree structure method.

3) Systems Modeling Language (SysML) review

Note: This section aims to review a modeling language called Systems Modeling Language (SysML). A simplified version of SysML known as SysML-lite is reviewed in this paper. The SysML-lite is provided in a Chapter 3 of book "A Practical Guide to SysML" by Sanford Friedenthal, Alan Moore and Rick Steiner [8]. The diagrams in this review were generated by using Astah SysML [9] and Modelio Open Source 3.7 [10].

a) Introduction

SysML is a graphical modeling language for presenting an overview of a system that includes the structural composition, behavior, constraints and requirements of a system. SysML supports the analysis, specification, design, verification, and validation of complex systems. It is an extension of a subset of the Unified Modeling Language (UML) used in software engineering.

SysML aims to model the following aspects:

1. The structural composition of the system.
2. Interconnection between systems, subsystems, and components.
3. Exchange of messages between parts of the system.
4. The actions and behavior of the system and its components.
5. The parametric relationships of the properties of the system and its components.

b) SysML diagrams

SysML includes nine different diagrams, which are as follows:

1. Package diagram
2. Requirement diagram
3. Activity diagram
4. Sequence diagram
5. State machine diagram
6. Use case diagram
7. Block definition diagram
8. Internal block diagram
9. Parametric diagram

SysML-lite excludes the sequence diagram, the state machine diagram and the use case diagram of SysML. Furthermore, it only includes a subset of available language features. However, it still provides significant modeling capabilities.

BLOCK DEFINITION DIAGRAM

Blocks are the basic structural elements in SysML and are used to represent the components of a system such as hardware software, data, procedure, facility, or a person. Furthermore, a block can contain different compartments for holding the block features such as properties, operations, and constraints.

The block definition diagram, labeled *bdd*, is often used to describe the structural composition of a system. It shows the sets of blocks and its characteristics in a system. An example of the block definition diagram for an air compressor is shown in Figure 2. The figure shows the components of an air compressor system. The connector with black diamond at one end and arrow at another represents a whole-part relationship. The system is placed in the black diamond end and its components are placed at the arrow end.

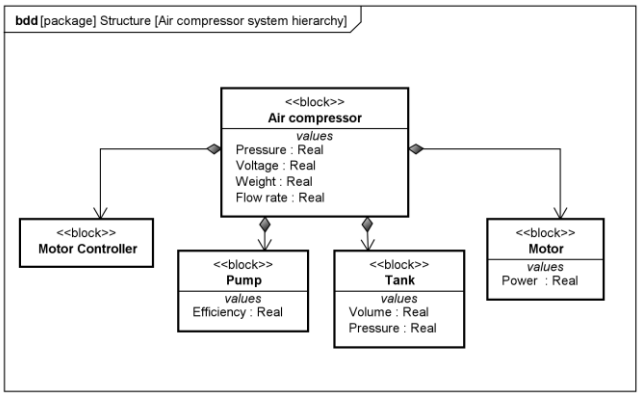


Figure 2. A block definition diagram for an air compressor.

INTERNAL BLOCK DIAGRAM

An internal block diagram, labeled *ibd*, in SysML presents the internal structure and connections of the components in a system. In this diagram, the interconnections between components are shown using ports and connectors. Ports are the interaction points on a block for the connection and specify component interfaces; and a connector is a line that connects the blocks in the internal block diagram. An internal block diagram of an air compressor is shown in Figure 3. The figure presents the interconnection and interactions between the components inside an air compressor.

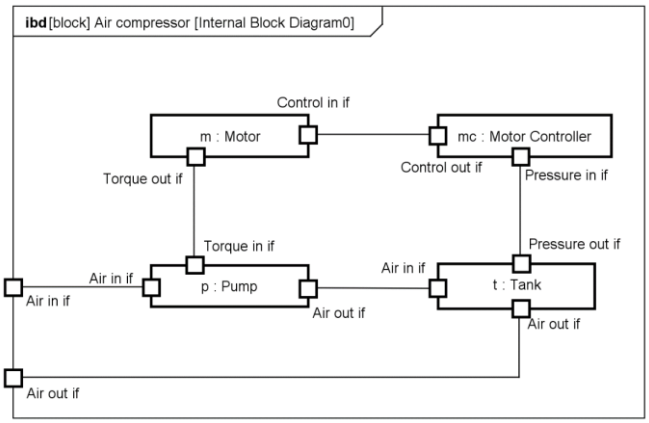


Figure 3. An internal block diagram of an air compressor.

REQUIREMENT DIAGRAM

Complex systems have a set of requirements that needs to be fulfilled for a system to function; and are presented in its specification document. A requirement diagram, labeled *req*, is used in SysML to show these sets of text-based requirements in a graphical model. Each requirement block in this diagram has compartments that displays the id of the requirement and text explaining the requirement. This diagram helps designers to create a design according to the requirements of the system and to verify the design later. In addition, it can be used for the system analysis during an operational period, to check if the system deviates from intended design for identifying risks in a system. Figure 4 shows a requirement diagram for an air compressor. The values for each requirement are not provided in the diagram and are replaced by X.

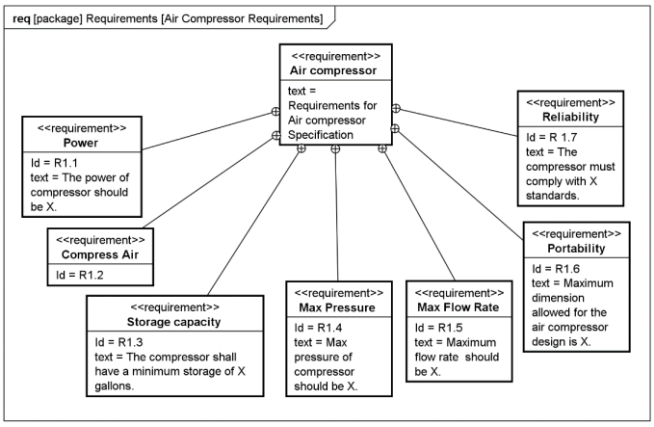


Figure 4. A requirement diagram for an air compressor.

ACTIVITY DIAGRAM

The activity diagram, labeled *act*, in SysML presents how an initialized process or activity is carried out inside a system. It shows all the components involved in the activity, the sequence of the interactions, the required inputs to the activity, and the output, which is produced from the activity. The symbols used in the activity diagram and their descriptions are presented in Table 2.

Table 2. The symbols and description of nodes used in the activity diagram.

Symbol	Description
	**Initial Node:** This symbol is used to indicate the starting point of the activity.
	Final Node: This symbol is used to indicate the ending point of the activity.
	Fork Node: This node is used to duplicate a flow of action into multiple parallel flows.
	Join Node: This node is used to join different multiple flows together into one.
	Action Node: This symbol is used to denote an action.
	Object Node: This symbol is used to denote the inputs and outputs of the activity.

Figure 5 shows the activity diagram for compressing air. At first, the total content area available for the activity diagram is partitioned depending on the number of subsystems or components, which are required for the activity and are labelled. An initial node is placed to denote the start of the activity. Then the action nodes are placed in a correct sequence in their respective component partition. Furthermore, the inputs required for the process and the outputs from the process are placed in an object node; and are connected to the action nodes. The control flows in the activity such as a connection between an initial node and a controller, are represented with a dashed line, while the action flows and object flows are represented with a solid line. A final node is then added to the control flow to denote the completion of the control activity. Thus, this diagram presents the sequence in which the action is carried in a system and the components involved in it.

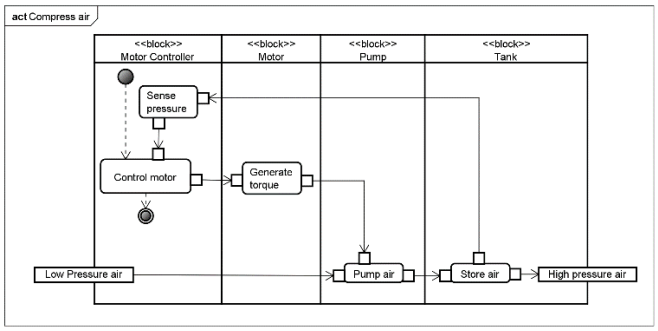


Figure 5. An activity diagram for compressing air.

PARAMETRIC DIAGRAM

Parametric diagrams, labeled *par*, in SysML are used to express constraints for supporting the engineering analysis of the system such as performance and reliability. Furthermore, it also helps to identify the critical performance properties of the system for design improvements. In a parametric diagram, a constraint block is used in the model that holds an equation or set of equations for the analysis. The properties or values that are required by the equations are then imported from the blocks in the block definition diagram. A parametric diagram for the flow rate analysis of the air compressor is shown in Figure 6. The equations for the analysis are not shown in the diagram for simplicity.

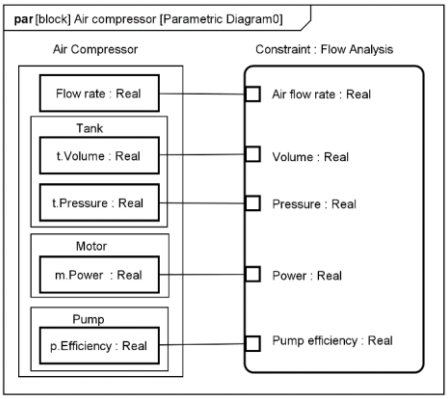


Figure 6. Parametric diagram for the flow analysis of Air compressor.

PACKAGE DIAGRAM

The SysML diagrams contain several model elements such as blocks, requirements, constraints as discussed in previous diagrams. As the modern systems are usually comprised of several components and functions, the number of model elements in a SysML model can get large. Thus, managing these vast numbers of elements is necessary; and for this purpose, packages are created in SysML. A package acts as a folder and is used to group similar model elements together. [8]

A package diagram, labeled *pkg*, in SysML displays all the packages within a system model. An example of a package diagram is shown in Figure 7.

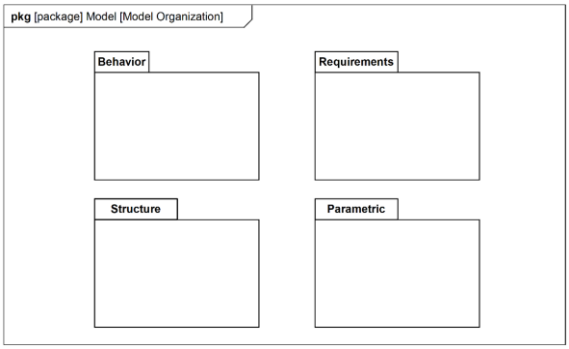


Figure 7. An example of a package diagram in SysML.

B. *Risk analysis methods review*

1) Introduction and selection of methods

Risk analysis methods aim to identify risks in a system to avoid hazards and accidents. As explained in the research background of this paper, the nature of risks is changing because of increasing component interactions. Most of the traditional risk analysis methods that are currently used for identifying risks in a ship system do not focus on potential issues due to component interactions. However, traditional risk analysis methods are still dominant in the risk analysis of the ship systems. Hence, this review aims to compare a widely used traditional method, which was developed for simpler systems of past and a modern method that was developed for identifying risks in complex systems.

The mostly used traditional risk analysis methods are Fault Tree analysis (FTA), Failure modes and effect analysis (FMEA) and Hazard and operability study (HAZOP). Thus, one of these methods will be compared with a modern method developed for identifying risks in complex systems known as System-Theoretical Process Analysis (STPA).

a) System's-Theoretical Process Analysis (STPA)

STPA, based on system's theory, aims to identify risks in a complex system. Instead of identifying risks by breaking down the system into component level, it uses a holistic approach and starts by identifying accidents and risks at the system level.

b) Fault Trees analysis (FTA)

FTA aims to identify all combinations of events that lead to a fault in a system. It is a top down approach, which uses logic gates to illustrate the combinations in a graphical model. [11]

c) Failure mode and Effect analysis (FMEA)

FMEA is a method used to identify faults and failure modes of components in a system. Furthermore, it also includes the effect and severity of faults. Unlike FTA, the result of this analysis is presented in a table. [11]

d) Hazard and Operability study (HAZOP)

HAZOP is a method that uses different guidewords such as "no" and "less" to identify potential deviations from intended or designed function in a system. The result of HAZOP includes the identified deviations, causes and consequences and the result is presented in a table. [11]

Based on the literature review [12], a general comparison of FTA, FMEA and HAZOP is presented in Table 3. The scale used in the comparison are Easy/ Moderate/ Difficult and Yes/No according to the context.

Table 3. A general comparison between FTA, FMEA and HAZOP [12].

Question	FTA	FMEA	HAZOP
How difficult is it to understand the method?	Moderate	Easy	Easy
How difficult is it to implement the method?	Easy	Easy	Easy
Is it possible to conduct without a team?	Yes	No	No
Is there any availability of software assistance for the analysis?	Yes	Yes	Yes
Does it analyze the combination of events for identifying fault	Yes	No	No
What is the result format?	Graphical model.	Table	Table

FTA is comparatively difficult than FMEA and HAZOP as it includes different scientific theories and principal such as logic theory, Boolean algebra and reliability theory. However, it analyzes the combination of events for identifying risks which is lacking in FMEA and HAZOP. Furthermore, the FMEA and HAZOP analysis requires a team and it lacks in analyzing the combination of events for identifying faults. Thus, FTA was selected as the traditional method to be compared with STPA.

2) Fault Trees Analysis (FTA)

Note: The FTA symbols presented in this paper were generated using Edraw Max 9.1 software [13].

a) Introduction

Fault Tree analysis is a traditional risk analysis method developed in 1962 by H. Watson and Allison B. Mearns of Bell Telephone Laboratories. It was developed for the U.S. Air force to evaluate Minuteman missile launch system. Later, this method was adopted and developed by a Boeing company, and since then many other industries have implemented FTA as a part of their hazard analysis process. [12]

FTA is a graphical model that determines how a combination of fault processes and component failures or even a normal process can lead to an undesired event. This undesired event can be an accident or hazard for a system. In qualitative FTA, several types of events are represented with different node shapes. Moreover, the diverse combinations of these events are then presented with Boolean logic gates and symbols in a tree-like structure.

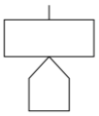
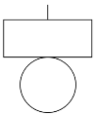
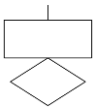
b) FTA building blocks

Different node types are connected to create an FTA diagram. Each node contains a rectangular block for texts and are interconnected by Boolean logic and symbols. There are four categories of node types in FTA, which are Basic Events (BE), Conditional Events (CE), Gate Events (GE), and Transfer Events (TE). [12]

BASIC EVENTS (BE)

This category consists of the normal events and failure events of the system that can lead to a hazard or fault. The symbols and descriptions of the basic events are presented in Table 4 [12].

Table 4. Symbols and descriptions of the basic events in FTA.

Type	Symbol	Description
Normal event		It is described as an event that occurs as intended or designed. Although the event is normal in an individual level, but when combined with other events can result in faults.
Primary failure event		It represents a basic failure event such as component failure that cannot be further developed.
Secondary failure event		It represents an undeveloped event. It can be undeveloped due to lack of information about the event or if it does not require further resolution.

CONDITIONAL EVENTS (CE)

Conditional events denote a condition that is required for some specific gate events to occur. A CE is represented by an ellipse and is attached to the gate events. A Conditional Event attached to an AND gate is shown in Figure 8. [12]

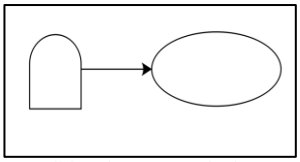


Figure 8. A conditional event attached to AND gate in FTA.

GATE EVENTS (GE)

In FTA, the events are linked with different logical operators known as gates. There are five different gate types in FTA and each of the gates represent a unique combination of events leading to the fault. Table 5 presents the different types of gate events used in FTA [12].

TRANSFER EVENTS (TE)

Transfer event is used to indicate a subtree branch that is used elsewhere in the tree. A triangle symbol, shown in Figure 9, is used to denote this combination in FTA. A Transfer In symbol is used in the place where the branch is getting imported and a Transfer Out symbol is then connected to a branch that is getting transferred which indicates that the branch is in use with another FTA. [12]

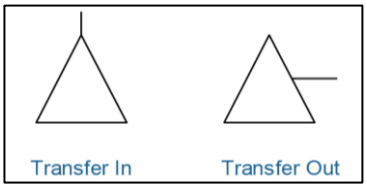
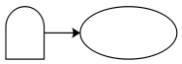
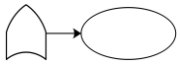
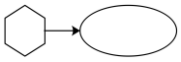


Figure 9. The symbols of Transfer events used in FTA.

Table 5. The symbols and description of different types of gates in FTA.

Type	Symbol	Description
AND Gate		This gate is used if the output event occurs only when several input events occur together.
OR Gate		This gate is used if the output event occurs when any of the input events occur.
Priority AND Gate		This gate is used if the output event occurs when all of the input events occur together but in a specific order or priority. The priority statement is placed in the conditional event symbol.
Exclusive OR Gate		This gate is used if the output event occurs when either of the input events occurs but not when all of the input events occur. The exclusivity statement is placed in the conditional event symbol.
Inhibit Gate		This gate is used if the output event occurs when the input event occurs, and a specific condition is satisfied. The condition is placed in the conditional event symbol.

c) Procedure

A Fault Tree is developed at different levels with branches. The basic steps for constructing a Fault Tree are as following [12]:

1. Review and understand the fault event.
2. Identify all the probable causes of this fault event and develop further if it is required.
3. Identify the relationship of the Cause-Effect events.
4. Structure the tree with appropriate gate events for identified input events.
5. Review for a possible repetition of events.
6. Move to the next fault and repeat the process.

d) Example of FTA

An FTA for motor overheating is presented in Figure 10.

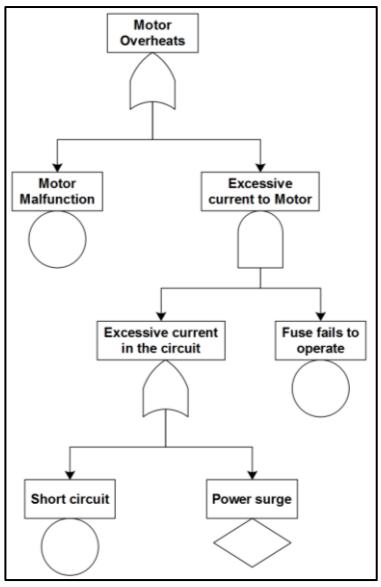


Figure 10. An FTA diagram of motor overheating [14].

3) Systems-Theoretical process analysis (STPA)

a) Introduction

STPA is a new hazard analysis technique developed in 2011 by Nancy Leveson (Professor of Aeronautics and Astronautics in MIT). Similar to other hazard analysis methods, it aims to identify the hazards and risks of the system. As traditional methods focus on identifying risks related to component failures and human errors, STPA also focuses on identifying other possible failures such as unsafe interactions among non-failing components, which can be caused from design flaws. [15]

STPA analysis is an iterative process and includes the following steps [15]:

1. Establish the foundation for the analysis. i.e. identify accidents and hazards, and prepare the control structure of the system.
2. Identify the potentially unsafe control actions in the system.
3. Create safety constraints and requirements for unsafe control action.
4. Determine how the unsafe control action could occur.

b) Procedure

Step 1: Establishing the foundation for the analysis.

STPA analysis starts by defining the accidents of the system Accidents can be defined as events that involve the loss or injury of humans in the system or loss of the system itself. After defining all the accidents of the system, hazards leading to each accident are identified. These identified accidents and hazards are reported in a table format. All hazards are then analyzed in detail; and safety constraints for eliminating or controlling them are created.

Next, a control structure of a system is prepared for analyzing all possible control actions in a system. As identifying accidents, hazards and safety constraints are common features of most of the hazard analysis techniques, this step makes STPA analysis unique from the rest. The control structure provides a graphical illustration of interactions among components and controllers.

For making a control structure, the main components of the system are first identified. Then, controllers and controlled components are classified among the components; and a control structure that shows the interactions between those components are created. A simple control structure for In-Trail procedure (ITP) is presented in Figure 11. However, the control structure can be prepared in detail if required. [15]

The control actions from the controllers in the control structure are presented with a solid line and the feedback received from the controlled components are presented with dashed line as shown in Figure 11.

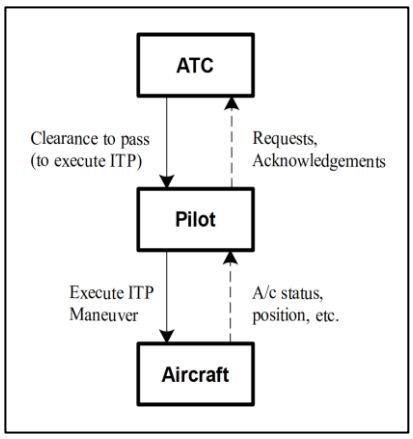


Figure 11. A simple control structure for In-Trail procedure (ITP) [15].

Step 2: Identifying the potential unsafe control actions.

After determining all possible control actions within the system, the unsafe control actions are identified using the guidewords. Standard guidewords used in STPA analysis are not providing the control action, providing the control action, providing the action too early or too late, and stopping the control action too soon or applying for too long [15].

All control actions are analyzed using the guidewords. For example, the analyst will check if providing or not providing the control action can cause any hazard in a system. The results of analyzed control actions with these keywords are then documented on a table.

Step 3: Creating safety constraints and requirements for unsafe control action.

After identifying all unsafe control actions of the system, safety constraints are implemented to control the hazard. For example, the safety constraints for unsafe control action "ITP executed when not approved" can be that "the flight crew must not execute the ITP until approved by the Air Traffic Control" [15]. This step is completed once safety constraints for all identified unsafe control actions are provided.

Step 4: Determining how the unsafe control actions could occur.

As only identifying unsafe control action in a system is insufficient for mitigating the risks in a system, how the unsafe control actions can occur in the system and what are its effects are determined in the final step of STPA analysis process. After knowing the causes of these unsafe control actions, again safety constraints will be established and enforced in a system to mitigate the risks. However, this step requires an input from experienced experts, as they are the one who can identify how these unsafe control actions can happen in a system. For example, an unsafe control action "Crew not providing manual braking in an aircraft when required" can result due to the following reason:

"The crew incorrectly believes that the autobrake feature is armed and will be engaged. This can happen due to a mistake of the crew or system design error such as multiple and conflicting messages, and alarm fatigue". [15]

Finally, the STPA analysis is completed after the safety constraints to control the causes of unsafe control actions, are created and enforced.

III. Discussions and Possible Solutions

The Tree structure method successfully presents the structural composition of the system However, it fails to provide the behavior or requirements, which is very important for understanding a complex ship system. SysML on the other hand, can present the structural composition of a system, requirements, and behavior of components. Furthermore, it also provides a diagram that can be used as a tool for conducting the engineering analysis of a system. The internal structure of a system, which is presented in an internal block diagram in SysML, helps to understand the connection and interactions between components, which is not provided by the Tree structure method. However, with increased capabilities and detailed modeling, the level of complexity of the method also increases. Furthermore, the time required for the analysis is also much higher than the Tree structure method.

Similarly, traditional risk analysis methods such as FTA are still dominant in marine industry. The review shows that the FTA is a simple and effective method for systems when the focus is on component failures and the combination of events in system leading to the fault. However, the concern with FTA is that it does not consider all type of risks in the system but only covers the major risks that are known to the analysts. As a result, they lack in analyzing most of the possible risks due to component interactions, which is growing with time in complex ship systems and should not be neglected. However, STPA analyzes a higher number of possible risks due to control actions i.e. component interactions and human errors. As the implementation of technology and autonomous functions in vessels will result in increased human design errors, FTA lacks to analyze those issues, where STPA on the other hand identifies most of the design errors and provide constraints to mitigate them. Furthermore, STPA analysis provides a systematic approach for identifying and mitigating risks. The STPA can be also applied during the early phase of a system design to guide the design process ensuring a safer design of a system.

As the overall functionality of SysML and STPA seems to be better than traditional methods, improving the drawbacks of these methods are important. The drawbacks of SysML and STPA identified in the review were the higher complexity of method and implementation time. The complexity of method can get better with several practices. Furthermore, the software tools for aiding the implementation process have just been developed, thus the tools will be further improved in the future. However, the analysis time consumption is also an important criterion for industries as they mostly have limited time resources because of increasing competition in the market. Some viable solutions to improve these drawbacks of SysML and STPA are presented below:

Possibility of creating a database in a STPA and SysML software tools.

A feature of creating a database is widely used by modern software's in different fields. For example, in 3D modeling, a database is created which stores all the models created and uploaded in the software, which then allows other users to download it afterwards instead of creating the same model again. Hence, in SysML a database containing all modeling elements such as blocks, requirements and constraints can be created which can be utilized to model another similar vessel or system. Similarly, in STPA, some of the hazards can be very similar between vessels or systems. Hence, a database that stores the elements such as control structure can be created.

A database has a potential to reduce the modeling and risk analysis time consumption. Furthermore, downloading complex elements instead of creating them can reduce the complexity of method.

Schematic layout of the system under assessment in a modeling tool.

One of the limitations identified during this research was the unavailability of the layout of the system being analyzed inside the tool itself. The analyst must check the layout of the system constantly for generating SysML diagrams and control structure in STPA. It will be easier if the tool contains a separate window that can be toggled on/off to display the schematic layout of the system. The analyst can then toggle on the window whenever he requires during the modeling process.

IV. Research Conclusions

The complexity in ship systems is further increasing. Traditional methods were not designed to handle complex ship systems since they were designed for the relatively simpler systems of the past. Although they have been modified to adapt current systems, they still lack in some extent to present some important information's about the system.

Based on the review, Table 7 and Table 8 present the main research conclusions of modeling approaches and risk analysis methods respectively. The scale used in the conclusion tables is provided in Table 6.

Table 6. The scale used in conclusion tables.

None
Low
Average
High
Very high

Table 7. The research conclusions of the modelling approaches review.

Question	Tree structure method	SysML
What is the method's complexity?	Low	High
How much time is required for the method implementation?	Low	Very high
What is the level of functionality?	Low	High
How suitable is the method for modeling a complex ship system considering the results?	Low	High

The research concludes that SysML is more complex and time consuming than the Tree structure method. However, unlike the Tree structure method, SysML models several aspects in a system such as behavior, requirements and support for engineering analysis. Hence, the functionality of SysML is significantly higher than the Tree structure method. Thus, considering the strengths and drawbacks, SysML is more suitable than the Tree structure method for modeling a complex ship system.

Table 8. The research conclusions of the risk analysis methods review.

Question	FTA	STPA
What is the complexity of the method?	Average	High
How much time is required for the method implementation?	Average	Very high
What is the level of functionality?	Average	High
What is the level of support for a systemic and systematic analysis?	Average	High
How suitable is the method for analyzing risks in a complex ship system considering the results?	Average	High

Similarly, STPA is more complex and time consuming than FTA because STPA follows a systemic approach that is different than most of the traditional risk analysis methods, and the analysis is more detailed in comparison. However, the functionality of STPA is better than FTA, which is very important for safety-critical systems. Although both are good at identifying risks due to the component failures, STPA is better at identifying risks due to the component interactions and human errors. In STPA, all possible interactions between components and controllers are analyzed, whereas in FTA the analysis depends on the preference and knowledge of the analysts. Thus, it is possible that the analysts conducting FTA will neglect some major risks and many minor risks due to the component interactions. Furthermore, both methods are systematic if the implementation process is followed correctly; but a systemic FTA of a complex ship system, with several sub-systems and the components, will result in large diagrams, which will be difficult to manage. Considering the strengths and drawbacks of each method, the research concludes that STPA is better than FTA.

However, it must be also considered that for some companies, the available resources for an analysis such as human resources, time resources and financial resources for the modeling and risk analysis of a system can be limited. In that case, traditional methods, the tree structure method and FTA will be more effective than SysML and STPA unless the implementation process of SysML and STPA are improved.

V. FUTURE RESEARCH POSSIBILITIES

This chapter suggests some future research possibilities to improve the research further.

Research on method's adaptation to the design changes. A ship system's design has been evolving in the past, and with ongoing autonomous ships projects, systems will keep evolving in the future. As the modeling and risks analysis of complex ship systems are lengthy processes, implementing the methods again from scratch after every design change can be tedious and costly. It would be beneficial for the companies and analysts if the earlier models could be modified according to the design changes. In that case, a version control system that keeps track and can manage earlier versions is also required. Hence, a study about the possibility of method is adapting to the design changes should be researched in future.

Review of methods with the consideration of probability. As mentioned in the limitations to this paper, probabilistic methods were not considered for the review in this research due to the lack of data about the failure of ship systems. However, the feature of assessing the probability of occurrence for risks in ship systems is very important as it helps to have more focus on critical risks. As a result, it will increase the effectiveness of the risk analysis method and modeling approach as more resources can be allocated for critical risks or elements in the system. Hence, a review including the probabilistic methods can be viable if data about ship systems can be accessed.

Review and comparison of the methods with a case study. The review of methods in this paper are based on the literatures review. A better comparison results can be achieved if these methods are implemented in a case study and feedback from experts are collected. Thus, a case study where these methods are applied to a complex ship system should be conducted and analyzed in future.

ACKNOWLEDGEMENT

This research is a part of Design for Value (D4 Value) program and the RESET project. The D4 Value program is partially funded by Tekes. RESET is partially supported by the European Union's Horizon 2020 Research and Innovation Programme RISE under grant agreement no. 730888 (RESET).

REFERENCES

[1] MUNIN, "Research in Maritime Autonomous Systems Project Results and Technology Potentials," 2016. [Online]. Available: http://www.unmanned-ship.org/munin/wp-content/uploads/2016/02/MUNIN-final-brochure.pdf. [Accessed 22 03 2018].

[2] AAWA, "Remote and Autonomous Ships - The next steps," 2016. [Online]. Available: http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf. [Accessed 27 March 2018].

[3] N. G. Leveson, M. V. Stringfellow and B. D. Owens, "" Safety-Driven Design for Software-Intensive Aerospace and Automotive Systems"," Institute of Electrical and Electronics Engineers, 2010.

[4] Y. Grobshtein, V. Perelman, E. Safra and D. Dori, "Systems Modeling Languages: OPM Versus SysML," 2007.

[5] S. Friedenthal, A. Moore and R. Steiner, "Getting Started with SysML," in *Practical Guide to SysML - The systems Modeling Language* , 2015, pp. 31-51.

[6] A. P. Sage and J. J. E. Aarmstrong, "Tree structure," in *Introduction to Systems Engineering*, John Wiley & Sons, 2000, p. 214.

[7] A. J. Brown, "Application of Operational Effectiveness Models in Naval Ship concept exploration and design," *Ship Science & Technology,* vol. 7, no. 13, pp. 9-21, 2013.

[8] F. Sanford and C. Oster, "Applying SysML and a Model-Based Systems Engineering Approach to a Small Satellite Design," in *Advances in Systems Engineering*, J. Hsu and R. Curran, Eds., American Institute of Aeronautics and Astronautics, 2016.

[9] Apache, *Astah SysML 1.4,* Apache Software Foundation, 2016.

[10] M. Community, *Modelio 3.7,* 2018.

[11] K. Alverbro, B. Nevhage and R. Erdeniz, "Methods for Risk Analysis," US AB, Stockholm, 2010.

[12] C. A. Ericson, Hazard analysis techniques for system safety, 2nd ed., New Jersey: John Wiley & Sons, 2015.

[13] Edrawsoft, "Edraw Max 9.1," 2018.

[14] C. Sundararajan, "cedengineering- Fault Tree Construction in Reliability Engineering," 2012. [Online]. Available: https://www.cedengineering.com/userfiles/Construction%20in%20Reliability%20Engineering.pdf. [Accessed 5 July 2018].

[15] N. Leveson, An STPA Primer, 2013.